

Appl. No. 09/903,612
Amdt. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

Amendments to the Drawings

Please remove current drawing sheet 6 that has been included in error. The Applicant notes that both drawing sheets 5 and 6 contain an identical figure, namely Fig. 5 and that only one should be included in the application.

Appl. No. 09/903,612
Amdt. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Drawings

In the Office Action, the Examiner objected to the drawings under 37 CFR 1.84(u), as sheets 5 and 6 of the drawings both contain views labeled as Fig. 5. As instructed above, the current drawing sheet 6 is to be removed from the application. The Applicant notes that the duplicate Fig. 5 (i.e. sheet 6) was submitted in error.

The drawings were also objected to under 37 CFR 1.83(a). The Applicant respectfully disagrees, and believes that the features described in claim 7, namely that the packet interceptor is a driver included in a kernel of an operating system in computer readable medium of the system, do not add additional features. The packet interceptor has been identified in Figure 3 by numeral 36. The limitation that the packet interceptor is a driver only limits the type of module that numeral 36 embodies and does not add an additional feature.

The packet interceptor is part of the IPsec module 34, which is part of the layer 28. The limitation that the driver is included in a kernel of an operating system in computer readable medium only dictates the location of the packet interceptor. The Applicant notes that page 3, line 22-26 of the description states that each of the correspondents has a computer readable medium and executes an operating system. These structures are well known components in devices such as those used by the correspondents. Since the limitations of claim 7 were part of the original application, support exists for these limitations, and the Applicant notes that the description has been amended for conformity (see remarks regarding claim rejections below). Therefore, it is believed that the drawings comply with 37 CFR 1.83(a).

Claim Objections

The Examiner objected to claims 5 and 10 due to several informalities. The expression "An system" on line 1 of claim 5 has been amended to read "A system"; and the expression "An method" on line 1 of claim 10 has been amended to read "A method". The word "to" has been inserted on line 17 of claim 10 as suggested by the Examiner, and the comma on line 9 of claim 10 has been replaced with a semicolon. The expression "having the step of" on line 3 of claim

Appl. No. 09/903,612

Andt. Dated: April 22, 2005

Reply to Office Action of: October 25, 2004

10 has been amended to read "comprising the steps of". The Applicant notes that the formulating of claim 6 has been corrected as reflected in the above amendments to the claims, without amending the claim itself. The Applicant also notes that the term "protocol" on line 4 of claim 1 has been replaced with the term "network", consistent with the terminology of the remainder of claim 1.

Claim Rejections

The Examiner rejected claim 7 under 35 U.S.C. 112, first paragraph, for failing to comply with the enablement requirement. The paragraph between page 4, line 23 and page 5, line 10 of the specification has been amended to comply with 35 U.S.C. 112. Specifically, the expression "included in a kernel of the operating system of the computer readable medium of the system" has been inserted at line 27 of page 4, between "driver" and "placed". Since this limitation was originally present in claim 7, no new subject matter has been added. The Applicant notes that the above amendment does not add any additional features to the invention, but only describes a particular implementation and location in the system.

The Examiner rejected claims 4, 5, 8 and 9 under 35 U.S.C. 112, second paragraph, as being indefinite.

In claim 4, the expression "the step of examining" has been amended to read "the step of determining whether to process said at least one data packet by examining", which was introduced in claim 1. The Applicant notes that the expression "said data packet includes further the steps of:" on line 2 of claim 4, has been amended to read "said data packet further includes the steps of:".

In claim 5, the expression "at least one data packet" on line 5, has been amended to read "at least one encapsulated IP packet", to provide the necessary antecedence for the expression "said encapsulated IP packet" on line 6. The expression "said cryptographic transformations" has been amended to read "said cryptographic functions" consistent with the expression "providing cryptographic functions" on line 2 of claim 5.

In claim 8, the expression "cryptographic transformations" has been amended to read "cryptographic functions", consistent with the terminology of claim 5.

Appl. No. 09/903,612
Amdt. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

In claim 9, "said" has been inserted between "wherein" and "secure" on line 1, "of said system are" has been inserted between "is" and "provided" on line 2, and "is" removed from line 2. The expression "for secure communications between correspondents of said system" has been inserted on line 1 of claim 5 between "packets" and "by", thereby providing the necessary antecedence for the terminology used in claim 9.

The Examiner has rejected claims 1-3, 5, and 8-10 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication No. 2002/0184487 to Badamo et al. The Applicant respectfully traverses this rejection.

The present invention teaches how to add IPsec tunneling transparently to point-to-point protocol (PPP) datagrams. Specifically, what has been described, and claimed, is to protect an IP packet inside an outbound PPP packet by placing the IP packet inside an IPsec tunnel inside the PPP packet. Similarly, on inbound traffic, the IP packet is extracted from an IPsec tunnel within an inbound PPP packet. In adding IPsec capability to an existing PPP implementation, no modifications are required to the operating system, or the addition of hardware.

As shown in Figures 4 and 5 and described on page 5, line 20 to page 6, line 12, PPP datagrams are intercepted both inbound and outbound of the network stack. The PPP datagrams have encapsulated data packets that are en route along the network stack. The PPP datagrams are decapsulated to retrieve the encapsulated data packets and these packets are examined to determine whether to process the same. The packets are then modified to provide cryptographic functions (e.g. IPsec) and encapsulated for transmission to another layer in the network stack.

Therefore, the PPP datagrams are decapsulated to reveal the encapsulated data packets therein and if processing is required, cryptographic functions are added thereto and then encapsulated within the PPP header and trailer to create a new PPP datagram. Since the encapsulation results in the original IP packet being hidden or included inside a PPP datagram, the IP header of the tunnel mode protected packet provides the necessary routing information, enabling the packet to travel through a communication network without revealing the final destination stored in the original IP packet header (which is encapsulated with the cryptographic functions). Once the encapsulated IP packets reach their destination, the encapsulation header

Appl. No. 09/903,612
Amdt. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

can be removed and the original IP packet header used to route the packet to its final destination.

Claims 1, 5 and 10 clearly describe the above features.

Badamo teaches a network gateway device with a network physical interface for receiving and transmitting data and for receiving packets for transmission and forwarding packets from received data. A packet processor includes an ingress processing security subsystem with a decryption processor for decrypting packets and an egress processing security subsystem for encrypting packets. Therefore, Badamo provides separate incoming and outgoing security subsystems.

As described on page 4, column 1, lines 15-54 (which the Applicant notes has been cited by the Examiner *inter alia*, Badamo teaches the operation of the ingress and egress subsystems. Each subsystem is responsible for its respective processing of packets, whether they are incoming or outgoing. For example, the ingress subsystem processing incoming packets and includes one of protocol translation, decapsulation, decryption, etc. The ingress subsystem is configured to handle one of the above operations as part of the incoming processing. However, Badamo does not teach protecting an IP packet inside a PPP packet by encapsulating the IP packet and applying cryptographic functions which is placed within the PPP packet. Badamo is entirely silent in that regard. Badamo is concerned with the separate processing of outbound and inbound packets using separate subsystems. Badamo is not concerned with transparently protecting a data packet using, e.g., IPsec capability in a PPP implementation without requiring modifications to the operating system. On the contrary, if Badamo wishes to use IPsec, such capabilities would be configured in the ingress and egress subsystems as desired.

The Applicant believes that the Examiner has misconstrued the teachings of Badamo. Regarding claim 1: 1) Badamo does not examine the packets once they are decapsulated to determine whether they are to be processed and 2) does not teach modifying a decapsulated packet to provide cryptographic functions and encapsulating the modified packet for transmission. The Examiner has taken a series of optional features that have merely been mentioned in Badamo, and pieced them together, without properly appreciating the nature of Badamo's teachings and how Badamo's system actually operates.

Therefore, the Applicant believes that Badamo fails to teach the method recited in claim 1,

Appl. No. 09/903,612
Amtd. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

and as such, claim 1 clearly and patentably distinguishes over Badamo, and is in condition for allowance. Claims 2-4 are either directly or indirectly dependent on claim 1, and therefore, are also believed to distinguish over Badamo.

Claim 5 describes a system suitable for implementing the method of claim 1, and therefore similar arguments apply with respect to Badamo. Claims 6-9 are either directly or indirectly dependent on claim 5, and as such, are also believed to distinguish over Badamo.

Claim 10 describes a method similar to claim 1, directed to providing a cryptographic system for communication between correspondents in a communication network. Claim 10 provides similar processing of the data packets as claim 1, therefore, similar arguments apply.

Accordingly, the Applicant believes that claim 10 also distinguishes over Badamo.

The Examiner has rejected claim 4 under 35 U.S.C. 103(a) as being unpatentable over Badamo in view of US. Patent No. 6,438,612 to Ylonen. Although claim 4 is dependent on claim 1, the Applicant will show that the claims of the present application also distinguish over such a combination.

Ylonen teaches a system and method for enabling the identification of virtual networks and/or virtual routers in the course of tunneling data packets through a network. As indicated by the Examiner, Ylonen teaches checking header information of packets that are sent in the communication system described therein. However, Ylonen does not teach transparently protecting a data packet using, e.g., IPsec capability in a PPP implementation without requiring modifications to the operating system. There is no suggestion in Ylonen to implement such functionality. Ylonen is silent in that regard. Ylonen fails to teach the missing elements not found in Badamo, and there is no suggestion that would enable a person skilled in the art to achieve the system and methods described in claims 1, 5 and 10.

Therefore, the Applicant believes that the combination of Ylonen and Badamo does not teach all of the elements of claims 1, 5, and 10, nor is there any suggestion of such an implementation in either reference. Accordingly, claims 1-10 are believed to patentably distinguish over the combination of Ylonen and Badamo.

Appl. No. 09/903,612

Amdt. Dated: April 22, 2005

Reply to Office Action of: October 25, 2004

The Examiner has rejected claims 6 and 7 under 35 U.S.C. 103(a) as being unpatentable over Badamo in view of U.S. Patent Publication No. 2004/0054794 to Lantto et al. Although claims 6 and 7 are dependent on claim 5, the Applicant will show that the claims of the present application also distinguish over such a combination.

Lantto teaches a system and method for Internet Protocol data communications. Lantto provides a way to remotely and securely access a computer in a private network. A remote access login system is profiled for accessing the private network via a pseudo-connectionless technology device.

As indicated by the Examiner, Lantto describes a driver included in a kernel of an operating system. However, Lantto does not describe encapsulating a data packet to provide cryptographic functions and encapsulate the protected packet in a PPP packet. Lantto, therefore, does not teach the missing features of claims 1, 5 and 10, not found in Badamo. The Applicant believes that there is nothing in the teachings of Lantto that would suggest the Badamo's teachings could be modified to arrive at the system of claim 5 or methods of claims 1 and 10.

Therefore, the Applicant believes that the combination of Badamo in view of Lantto does not teach every element of claims 1, 5 and 10. Accordingly, claims 1-10 are believed to patentably distinguish over such a combination.

Summary

In view of the foregoing, claims 1-10 presented in this amendment are believed to constitute patentable subject matter under 35 U.S.C. 102 and 103, and comply with 35 U.S.C. 112, and as such, are in condition for allowance. The drawings and description are also believed to be in condition for allowance.

BEST AVAILABLE COPY

Appl. No. 09/903,612
Amdt. Dated: April 22, 2005
Reply to Office Action of: October 25, 2004

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: April 22, 2005

Blake, Cassels & Graydon LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164

JRO/BSL